DATA PROTECTION POLICY

1. Our aim

1.1 We want everyone who comes to The Green House for support, who works for our organisation, or supports our work to feel confident and comfortable with how any personal information they share with us will be looked after or used.

2. Related policies and procedures

- Data Retention Policy
- Data Breach Policy
- Client Privacy and Data Protection Statement
- Staff Data Protection Responsibilities Statement
- Website Privacy Statement

3. About our policy

3.1 The Green House has a legal obligation to comply with all appropriate data protection legislation, such as the EU General Data Protection Regulation (GDPR) and the Privacy and Electronic Communications Regulations (PECR).

3.2 The Green House also has a duty to comply with guidance issued by the Department of Health, the NHS executive, NHS Information Authority, Information Commissioner's Office, and other relevant advisory groups.

3.3 In order to carry out our responsibilities The Green House needs to collect and use certain types of information about our service users or other individuals ("data subjects") who come into contact with our organisation. This personal information will be dealt with appropriately and responsibly whether collected on paper, stored in a computer database, or recorded on other material.

3.4 The Green House is the Data Controller as defined by the GDPR, which means that the organisation determines what purposes personal information held will be used for. It is also responsible for notifying the Information Commissioner of the data it holds or is likely to hold, and the general purposes that this data will be used for.

3.5 The Green House may need to share data with other agencies such as, but not necessarily limited to, a local authority, regulated health service providers, police, Inland Revenue and other Government bodies.

4. Data protection terms and definitions

4.1	Personal data	Any information relating to a natural person (the "Data Subject") who may be identified directly or indirectly from that information.
4.2	Sensitive data	A special category of personal data relating to a person's racial or ethnic origin, their politics, religious beliefs, physical or mental health, sexual orientation, or trade union affiliation.
4.3	Data user	Those involved in the processing of personal data.
4.4	Data controller	The organisation which collects and determines the use of personal data.
4.5	Processing	Any operation performed on personal data such as collection, storage, retrieval, transfer or transmission, dissemination, deletion/destruction, or adaptation or alteration.
4.6	Consent	The consent of a data subject means any freely given, specific, informed and unambiguous indication by statement or clear affirmative action, signifying agreement to the processing of their personal data.
4.7	Data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data.

5. Data protection principles

5.1 The Green House is committed to ensuring that personal data is treated lawfully and correctly. Anyone processing personal data must comply with the principles of the GDPR. Specifically, the GDPR requires that personal information:

- Shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met
- Shall be obtained only for one or more of the purposes specified in the GDPR, and shall not be processed in any manner incompatible with those purposes
- Shall be adequate, relevant and not excessive in relation to those purposes
- Shall be accurate and, where possible, kept up to date
- Shall not be kept for longer than is necessary
- Shall be processed in accordance with the rights of data subjects under the GDPR
- Shall be kept secure by the Data Controller who takes appropriate technical and other measures to prevent the unauthorised or unlawful processing or accidental loss or destruction of, or damage to, personal information
- Shall not be transferred to a country or territory outside European Economic Area unless that country or territory ensures an adequate and approved level of protection for the rights and freedoms of individuals in relation to the processing of personal information
- Any data used for non-operational analysis purposes will be fully anonymised

6. Collecting and processing data

6.1 The Green House will, through appropriate management and strict application of criteria and controls:

- Observe fully conditions regarding the fair collection and use of information
- Meet its legal obligations to specify the purposes for which information is used
- Collect and process appropriate information, and only to the extent that it is needed to fulfill its operational needs or to comply with any legal requirements
- Ensure the quality of information used
- Ensure that the rights of people about whom information is held, can be fully exercised under the GDPR. These include:
    - The right to be informed that processing is being undertaken
    - The right of access to one's personal information
    - The right to prevent processing in certain circumstances
    - The right to correct, rectify, block or erase information which is regarded as wrong or inaccurate information

6.2 When collecting personal data The Green House will ensure that the individual:

- Clearly understands why the information is needed
- Understands what it will be used for
- Understands what the consequences are should they decide not to give consent to processing
- Grants explicit consent, either written or verbal, for data to be processed
- Has given consent freely

7. Sharing data

7. 1 The Green House will ensure data subjects are made aware of, and give their explicit consent, to the circumstances where their information will be shared with a third party.

7.2 However, this is with the exception of the following circumstances where the law allows the disclosure of personal data (including sensitive data) without consent:

- Carrying out a legal duty or as authorised by the Secretary of State
- Protecting the vital interests of an individual, service user or other person
- The individual or service user has already made the information public
- Conducting any legal proceedings, obtaining legal advice or defending any legal rights
- Monitoring for equal opportunities purposes e.g. race, disability or religion
- Providing a confidential service where the individual or service user's consent cannot be obtained or where it is reasonable to proceed without consent e.g. where we would wish to avoid forcing stressed or ill individuals to provide consent signatures

8. Data security

8.1 Information and records relating to all data subjects will be stored securely and will only be accessible by authorised personnel for the performance of their specified roles.

8.2 The following security procedures will be implemented across The Green House:

- Desks – a clean desk policy applies across the organisation. All confidential and sensitive information should be locked away or disposed of when a desk is not in use.
- Secure storage – all cupboards and cabinets should be kept locked if they hold confidential information of any kind.
- PCs – data users must ensure that their monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.
- Portable devices – all laptops, phones, and tablets used for The Green House purposes should be password protected and used in line with The Green House IT policy.
- Training – everyone handling personal information will receive appropriate briefings and guidance to ensure their compliance with good data protection practice.
- Information – staff and volunteers must read and apply the procedures outlined in this policy and all related guidance and policies.

8.3 Information will be stored for only as long as it is needed, is relevant, or as required by statute, and will be disposed of appropriately i.e. the un-recoverable deletion of digital data and shredding of paper documents.

9. Right of access

9.1 All individuals and service users have the right to know what information The Green House holds about them.

9.2 In accordance with the GDPR, The Green House will respond to a Subject Access Request (SAR) within 1 calendar month, or if the request is particularly complex will advise the requester of the extended timescale.

9.3 The Green House will make no charge for responding to a Subject Access Request unless the request is complex, frivolous, or a repeat. Any charge will be sufficient to cover The Green House's direct cost of handling the request.

9.4 To make a formal Subject Access Request the individual should contact info@the-green-house.org.uk.

10. Right to be forgotten

10.1 All individuals and service users have the right to have their data deleted, formally known under the GDPR as the "Right To Be Forgotten" (RTBF).

10.2 The Green House will comply with a RTBF request without undue delay unless the data is being retained for statutory purposes or where The Green House can demonstrate that retention is necessary within the provisions of the GDPR (e.g. for the establishment, exercise, or defence of a civil claim).

10.3 To make a formal Right To Be Forgotten request the individual should contact info@the-green-house.org.uk.

11. Data breaches

11.1 In the event of a serious data breach The Green House will:

- Notify the Information Commissioner's Office (ICO) of a reportable data breach within the mandatory 72 hours of any personnel becoming aware of the breach.
- Will notify without undue delay all data subjects who have been, or could potentially be, adversely affected by the breach.

12. Quality assurance

12.1 The Green House is not of a sufficient size to legally require a formal Data Protection Officer. However, our internal Data Protection Lead plays an active role in:

- Monitoring our compliance with data protection legislation
- Advising The Green House on our data protection obligations, policies and procedures
- Acting as a contact point for any discussions with the ICO

12.2 The Green House will ensure that all staff and volunteers coming into contact with personal information understand that they are contractually responsible for following good data protection practice.

12.3 The Green House will regularly review and audit the ways it holds, manages and uses personal information.

12.4 This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the GDPR.

Date of last review: June 2018
Date of next review: June 2021